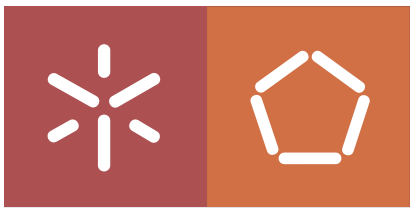

Universidade do Minho
Escola de Engenharia

Redes de Computadores

Relatório do Trabalho Prático nº4
Grupo 41

LEI - 2º Ano - 2º Semestre

Realizador por:

A98695	Lucas Oliveira
A89292	Mike Pinto
A96208	Rafael Gomes

Braga,
19 de maio de 2023

Conteúdo

Lista de Figuras

Capítulo 4

Acesso Rádio

Como pode ser observado, a sequência de bytes capturada inclui meta-informação do nível físico (radiotap header, radio information) obtida do firmware da interface Wi-Fi, para além dos bytes correspondentes a tramas 802.11. Selecione a trama de ordem XX correspondente ao seu identificador de grupo (TurnoGrupo, e.g., 11).

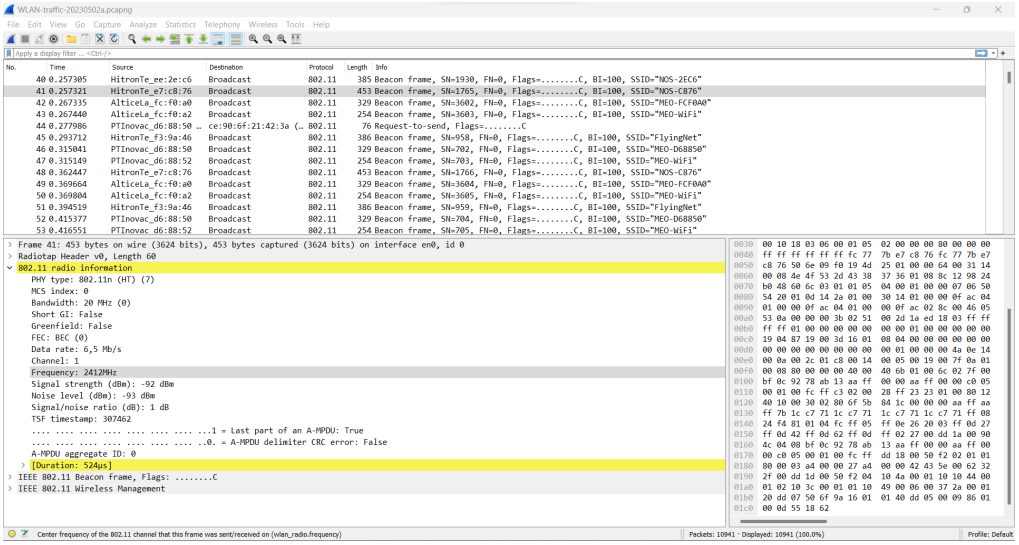

Figura 4.0.1: Trama de ordem 41 capturado pelo *"wireshark"*

Selecionamos a seguinte trama da figura 4.0.1, por sermos o grupo 41.

4.1 Pergunta 1)

Identifique em que frequência do espectro está a operar a rede sem fios, e o canal que corresponde essa frequência.

Após a análise da trama de ordem 41 da figura 4.0.1, verificamos que a rede sem fios está a operar na frequência de 2412 MHz do canal 1.

4.2 Pergunta 2)

Identifique a versão da norma IEEE 802.11 que está a ser usada.

Através da figura 4.0.1, podemos observar que a versão da norma a ser usada é a *802.11n*.

4.3 Pergunta 3)

Qual o débito a que foi enviada a trama escolhida? Será que esse débito corresponde ao débito máximo a que a interface Wi-Fi pode operar? Justifique.

Pelo campo *"Data rate"*, vemos que esta trama foi enviada por um débito de 6,5 MB/s, não sendo o máximo que a "interface" *Wi-Fi* pode operar. O debito máximo que a interface pode operar é 600 MB/s devido à norma *IEEE 802.11* a ser usada é o *802.11n*.

4.4 Pergunta 4)

Verifique qual a força do sinal (Signal strength) e a qualidade expectável de receção da trama, sabendo que:

A força do sinal da trama observada é de *-92 dBm* que indica que as hipóteses de se conseguir conectar são baixas.

Capítulo 5

Scanning Passivo e Scanning Ativo

Como referido, as tramas beacon permitem efetuar scanning passivo em redes IEEE 802.11 (Wi-Fi). Para a captura de tramas disponibilizada, e considerando XX o seu nº de TurnoGrupo (PLXX), responda às seguintes questões:

5.5 Pergunta 5)

Selecione uma trama beacon cuja ordem (ou terminação) corresponda a XX. Esta trama pertence a que tipo de tramas 802.11? Identifique o valor dos identificadores de tipo e de subtipo da trama. Em que parte concreta do cabeçalho da trama estão especificados (ver anexo)?

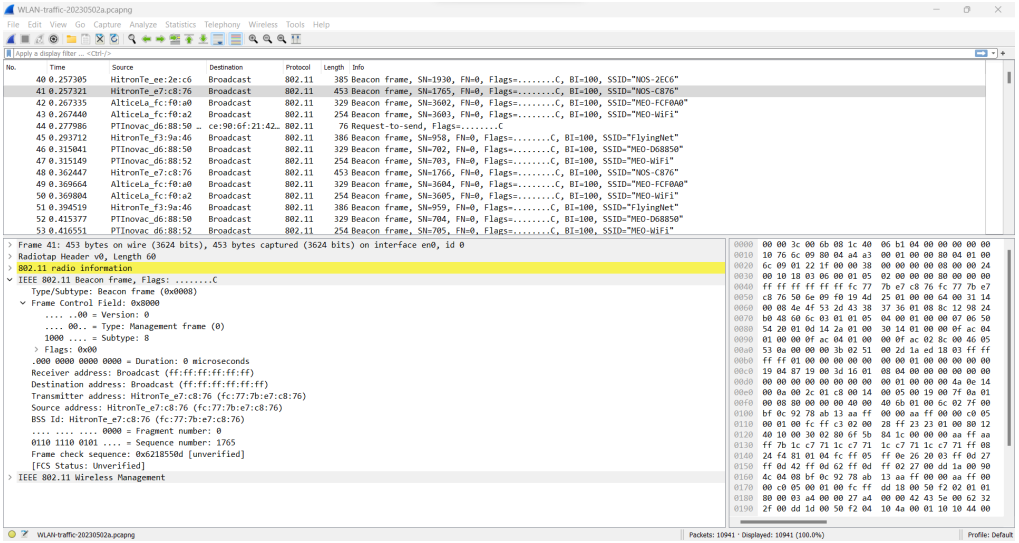

Figura 5.5.1: Trama beacon de ordem 41

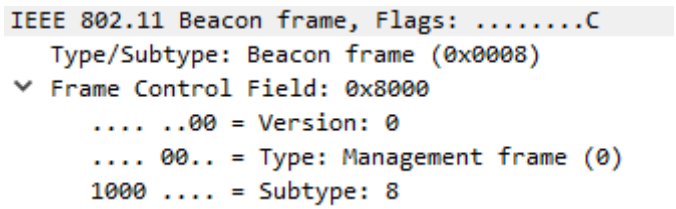

Figura 5.5.2: tipo e subtipo do *beacon* capturado pelo *"wireshark"*

Foi selecionado a trama de ordem 41, figura 5.5.1. O tipo de trama 802.11 a qual esta trama pertence é Beacon Frame.

Já pela figura 5.5.2, identificamos que o campo *type/subtype* possui o valor de *0x0008*. No campo *Frame Control Field* identificamos o valor do identificador *type* na trama possui valor 0, ou seja, identifica uma trama de *"management"*, já o seu subtipo tem o valor 1000 que identifica que se trata de *beacon*.

5.6 Pergunta 6)

Para a trama acima, identifique todos os endereços MAC em uso. Que conclui quanto à sua origem e destino?

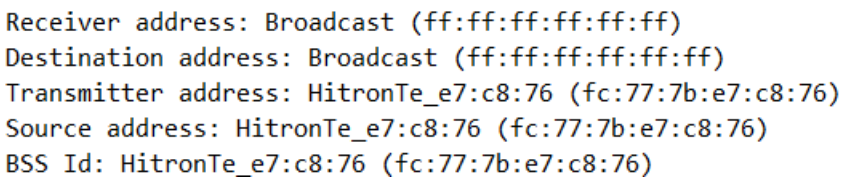

Figura 5.6.1: Endereços *MAC* capturado pelo *"wireshark"*

Pela figura 5.6.1 obtemos todos os endereços *MAC* em uso na trama. O endereço de origem é do equipamento que envia a trama, um *AP* (endereço *fc:77:7b:e7:c8:76*). Já o endereço de destino é *ff:ff:ff:ff:ff:ff* que representa que a trama tem destino todos os equipamentos da sua área, ou seja, esta trama tem como destino ser enviada em *Broadcast*.

5.7 Pergunta 7)

Verifique se está a ser usado o método de deteção de erros (CRC). Justifique. Justifique o porquê de ser necessário usar deteção de erros em redes sem fios.

Esta trama usa o método *CRC*, pois como podemos constatar na figura 5.5.1 o campo *Frame check sequence* apesar de possuir o valor de *Unverified*, o seu valor em *hexadecimal* difere de zero.

O uso de uma deteção de erros numa rede sem fios é necessário, pela confiabilidade da transmissão, pois as redes sem fios são suscetíveis a interferências e a ruídos, também pela qualidade de serviço por existir a possibilidade da perda de pacotes.

As tramas beacon permitem especificar parâmetros de funcionamento úteis para apoiar a operação e a gestão das ligações em fios.

5.8 Pergunta 8)

Uma trama beacon anuncia que o AP pode suportar vários débitos de base (B), assim como vários débitos adicionais (extended supported rates). Indique quais são esses débitos.

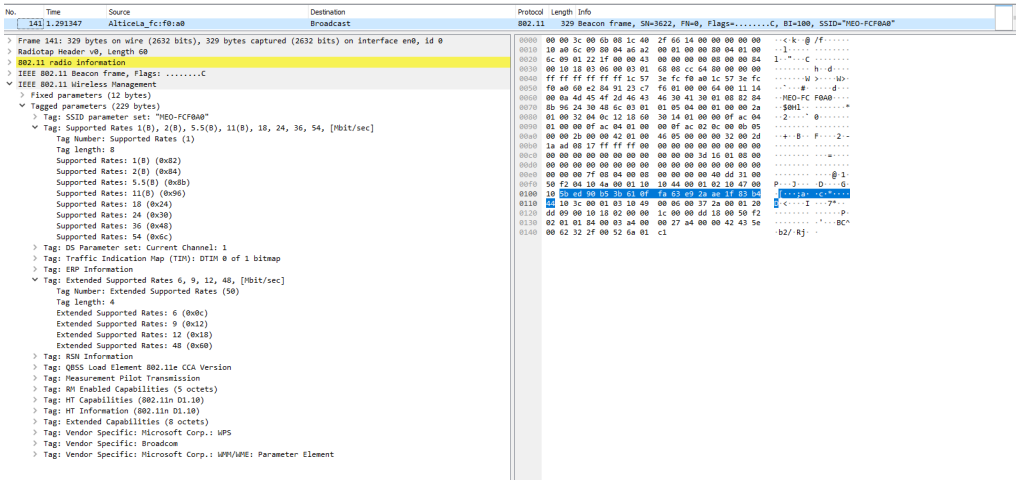

Figura 5.8.1: Débitos suportados pelo *Beacon* capturado pelo *"wireshark"*

Como a trama de ordem 41 não possuía o campo com a tag *extended supported rates*, selecionamos então respondendo a esta pergunta a trama de ordem 141.
Como podemos constar na figura 5.8.1 os débitos de base suportados pelo *Beacon* são 1, 2, 5.5, 11, 18, 24, 36 e 54 *Mbps* e os débitos adicionais são 6, 9, 12 e 48 *Mbps*.

5.9 Pergunta 9)

Qual o intervalo de tempo previsto entre tramas beacon consecutivas (este valor é anunciado na própria trama beacon)? Na prática, a periodicidade de tramas beacon provenientes do mesmo AP é verificada com precisão? Justifique.

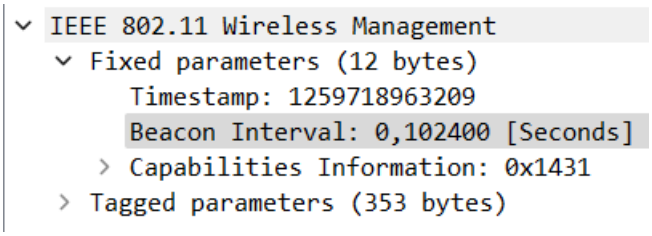

Figura 5.9.1: Intervalo de tempo entre tramas *beacon* consecutivas.

Temos que pelo campo *Beacon Interval* da figura 5.9.1, o tempo previsto entre tramas *beacon* consecutivas é de *0,102400* segundos. Examinando as tramas enviadas pelo mesmo *AP*, o valor do campo *Beacon Interval* é o mesmo. Por norma a periodicidade de tramas *beacon* é verificada. Isto deve-se ao facto que de um dos principais objetivos do *Beacon Interval* é alertar que a rede está ativa para sincronizar a transmissão dos dados.

5.10 Pergunta 10)

Identifique e liste os SSIDs dos APs que estão a operar na vizinhança da STA de captura. Explicite o modo como obteve essa informação (por exemplo, se usou algum filtro para o efeito).

Para listar todos os *SSID's* que estão operar na vizinhança *STA* utilizamos o filtro *(wlan.fc.type_subtype* $== 8$*)* obtendo os seguintes *SSID's*:

- TP-LINK_AP_AF08
- NOS-C876
- NOS-2EC6
- Masmorra do sexo
- MEO-WiFi
- MEO-FCF0A0
- MEO-D68850
- MEO-9E9BB0
- MEO-9BF2A0
- MEO-45BE30
- K6000 Plus
- FlyingNet

No trace disponibilizado foi também registado scanning ativo (envolvendo tramas probe request e probe response), comum nas redes Wi-Fi como alternativa ao scanning passivo.

5.11 Pergunta 11)

Estabeleça um filtro Wireshark apropriado que lhe permita visualizar todas as tramas probing request e probing response, simultaneamente.

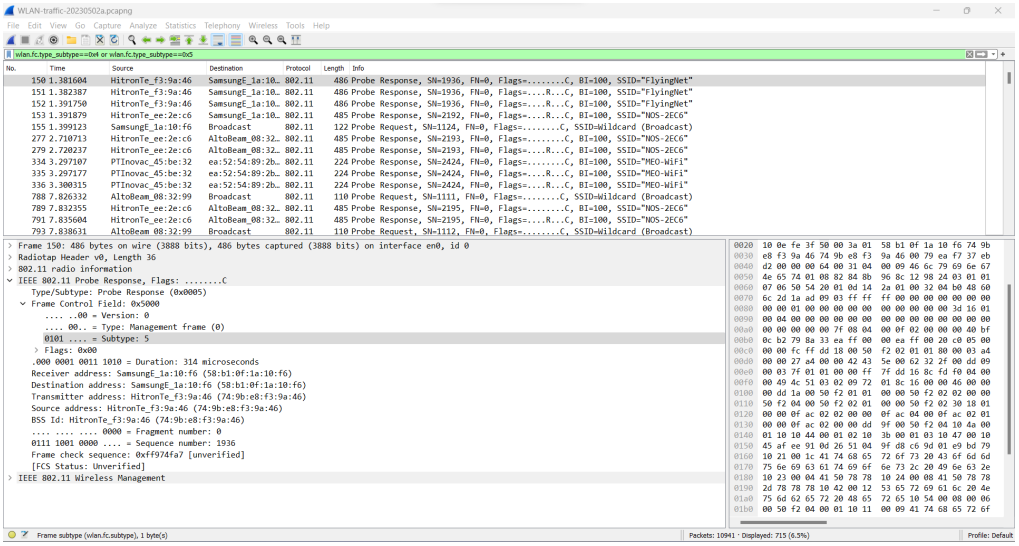

Figura 5.11.1: Filtro *wireshark* que permite observar tramas *probe request* e *probe response*

Sabemos que as tramas *probe request* e *probe response* possuem o *subtype 0x4* (100 em binário) e *0x5* (101 em binário) respetivamente. Então um filtro do wireshark que permita visualizar todas essas tramas seria do tipo:

$$wlan.fc.type\_subtype==0x4 \ or \ wlan.fc.type\_subtype==0x5$$

como podemos observar na figura 5.11.1.

5.12 Pergunta 12)

Identifique um probing request para o qual tenha havido um probing response. Face ao endereçamento usado, indique a que sistemas são endereçadas estas tramas e explique qual o propósito das mesmas?

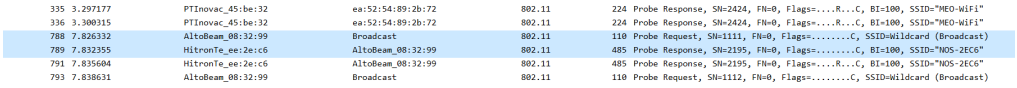

Figura 5.12.1: *Probing request* e o seu respetivo *probing response*

Como podemos observar na figura 5.12.1, é possível verificar que a trama 788 é um *probing request* e a trama 789 é o seu respetivo *probing response*.

A trama 788 é um *Broadcast* enviado pelo dispositivo*AltoBeam_08:32:99* que por sua vez é enviado para todos os equipamentos da rede, para encontrar um *AP*. Como resposta, surgiu a trama 789 que corresponde ao *HitronTe_ee:2e:c6*.

Capítulo 6

Processo de Associação

Numa rede Wi-FI estruturada, um host deve associar-se a um ponto de acesso antes de enviar dados. O processo de associação nas redes IEEE 802.11 é executada enviando a trama association request do host para o AP e a trama association response enviada pelo AP para o host, em resposta ao pedido de associação recebido. Este processo é antecedido por uma fase de autenticação. Para a sequência de tramas capturada:

6.13 Pergunta 13)

Identifique uma sequência de tramas que corresponda a um processo de associação realizado com sucesso entre a STA e o AP, incluindo a fase de autenticação.

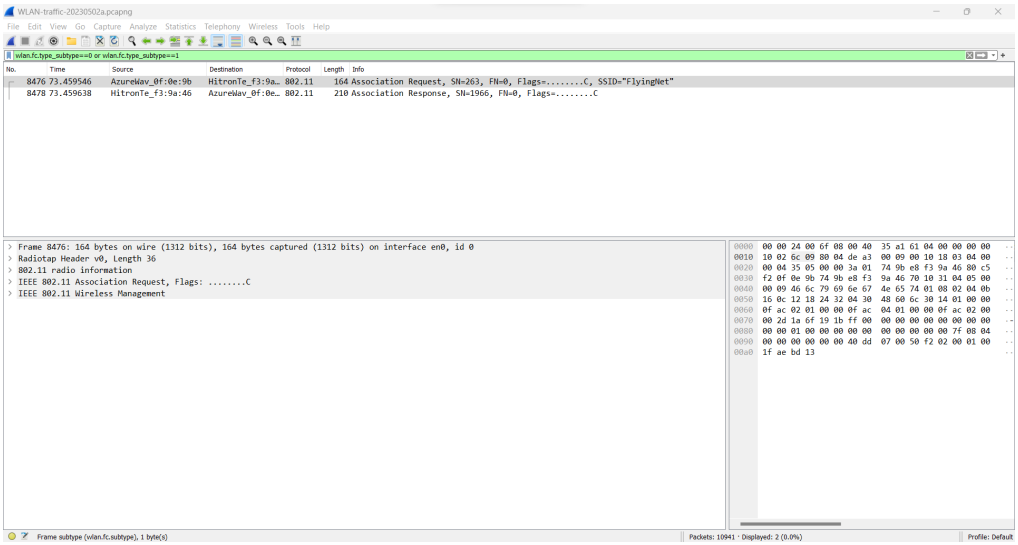

Figura 6.13.1: Tramas de *Association Request* e *Association Response*

Para identificar uma sequência de tramas que corresponda a um processo de associação entre um *STA* e um *AP* e sabendo que os *subtype* de tramas de *Association Request* e

Association Response é respetivamente *0x0* (0000 em binário) e *0x1* (0001 em binário), então executamos o seguinte filtro no *Wireshark*:

wlan.fc.type_subtype==0 or wlan.fc.type_subtype==1

Identificamos então as tramas de ordem 8476 e 8478, como podemos observar na figura 6.13.1.

8472	73.450730	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	802.11	70 Authentication, SN=262, FN=0, Flags=........C
8473	73.450745		AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b) (RA)	802.11	48 Acknowledgement, Flags=........C
8474	73.450775	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	802.11	70 Authentication, SN=1965, FN=0, Flags=........C
8475	73.450780		HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46) (RA)	802.11	48 Acknowledgement, Flags=........C
8476	73.459546	AzureWav_0f:0e:9b	HitronTe_f3:9a:46	802.11	164 Association Request, SN=263, FN=0, Flags=........C, SSID="FlyingNet"
8477	73.459553		AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b) (RA)	802.11	48 Acknowledgement, Flags=........C
8478	73.459638	HitronTe_f3:9a:46	AzureWav_0f:0e:9b	802.11	210 Association Response, SN=1966, FN=0, Flags=........C
8479	73.459643		HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46) (RA)	802.11	48 Acknowledgement, Flags=........C

Figura 6.13.2: Sequência de tramas correspondente a um processo de associação realizado com sucesso

Seguidamente analisamos a captura do *Wireshark* sem o filtro, figura 6.13.2. Identificamos então duas tramas de autenticação(tramas 8472 e 8474) e as respetivas tramas de *acknowledgement* (tramas 8473 e 8475). Identificamos também duas tramas de *acknowledgement* das tramas de *Association Request* e *Association Response* (tramas 8477 e 8479), concluindo então que o processo de associação foi realizado com sucesso sem qualquer tipo de erros. Resumindo, a fase de autenticação começa na trama 8472 e acaba na trama 8475 e seguidamente temos a fase de associação que começa na trama 8476 e 8479.

6.14 Pergunta 14)

Efetue um diagrama que ilustre a sequência de todas as tramas trocadas no processo

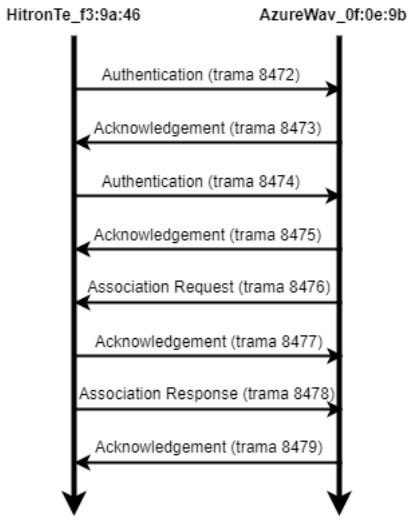

Figura 6.14.1: Diagrama a ilustrar a sequencia de tramas trocadas.

Efetuamos o diagrama da figura 6.14.1

Capítulo 7

Transferência de Dados

O trace disponibilizado, para além de tramas de gestão da ligação de dados, inclui tramas de dados e tramas de controlo da transferência desses mesmos dados.

7.15 Pergunta 15)

Considere a trama de dados nº8503. Sabendo que o campo Frame Control contido no cabeçalho das tramas 802.11 permite especificar a direccionalidade das tramas, o que pode concluir face à direccionalidade dessa trama, será local à WLAN?

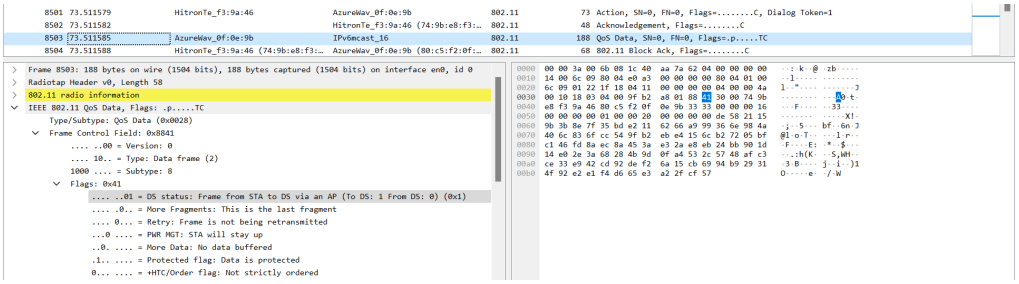

Figura 7.15.1: Endereços *MAC* da trama nº8503 capturado pelo *Wireshark*

Através da figura 7.15.1, podemos verificar que a direcionalidade da trama em causa toma a direção do *STA* para o *DS* através do *AP*. Relativamente, à rede *WLAN*, sabemos que um *AP* é um dispositivo central de uma *WLAN*, sendo assim, podemos concluir que será local, pois o endereço *MAC* da *source* corresponde ao *STA* e a *destination* ao *AP*.

7.16 Pergunta 16)

Para a trama de dados nº8503, transcreva os endereços MAC em uso, identificando quais os endereços correspondentes à estação sem fios (STA), ao AP e ao router de acesso ao sistema de distribuição (DS)?

```
Receiver address: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
Transmitter address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
Destination address: IPv6mcast_16 (33:33:00:00:00:16)
Source address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
BSS Id: HitronTe_f3:9a:46 (74:9b:e8:f3:9a:46)
STA address: AzureWav_0f:0e:9b (80:c5:f2:0f:0e:9b)
```

Figura 7.16.1: Endereços *MAC* da trama nº8503 capturado pelo *Wireshark*

Como consta na figura 7.16.1 o endereço *MAC* (*80:c5:f2:0f:0e:9b*) corresponde à estação sem fios (*STA*), o endereço (*33:33:00:00:00:16*) corresponde ao *AP*, por fim o endereço (*74:9b:e8:f3:9a:46*) corresponde ao router de acesso ao sistema de distribuição (*DS*).

7.17 Pergunta 17)

Como interpreta a trama nº8521 face à sua direccionalidade e endereçamento MAC?

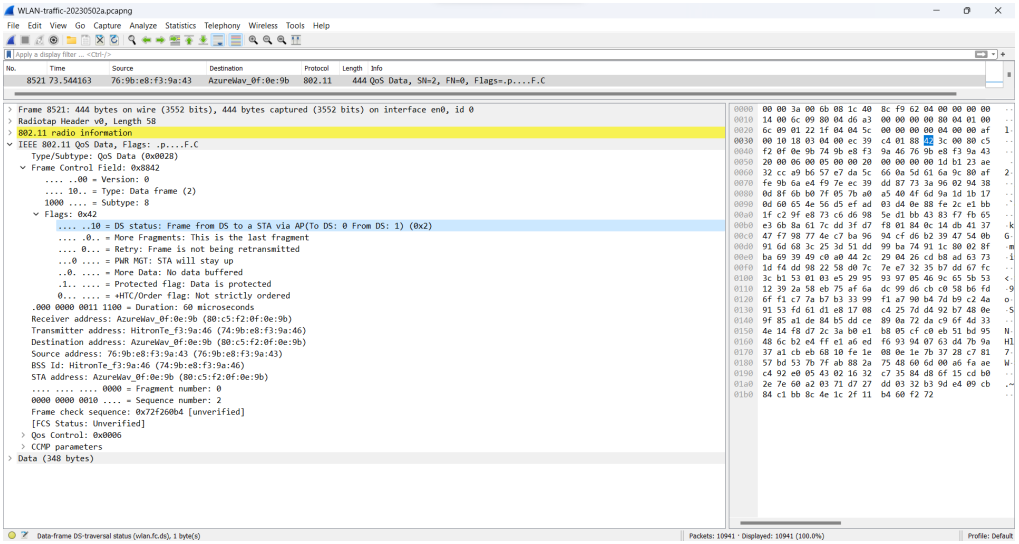

Figura 7.17.1: Caption

Como podemos verificar na figura 7.17.1, o campo *DS status* possui o valor de *"Frame from DS to a STA via AP(To DS: 0 From: 1)"*. Daqui concluímos que a trama vem de um host externo à rede, com endereço MAC *76:9b:e8:f3:9a:43*, onde o destino é o host *AzureWav_0f:0e:9b* (STA) com endereço MAC *80:c5:f2:0f:0e:9b* transmitido pelo *AP HitronTe_f3:9a:46* de endereço MAC *74:9b:e8:f3:9a:46*.

7.18 Pergunta 18)

Que subtipo de tramas de controlo são transmitidas ao longo da transferência de dados acima mencionada? Tente explicar a razão de terem de existir (contrariamente ao que acontece numa rede Ethernet.)

O subtipo de tramas transmitidas ao longo da transferência de dados acima mencionada é *QoS Data* cujo *subtype* tem valor de 8 (1000 em binário), como podemos verificar no campo *Subtype* do *Frame Control Field* na figura 7.17.1.

O subtipo de tramas QoS, *Quality of Service* são importantes em redes *Wi-fi* devido permitir a priorização de tráfego numa rede, dando a possibilidade de prealocar recursos e prioridade a um certo dispositivo devido a problemas de latência e largura de banda. Em redes *Ethernet* não existe tanto essa necessidade devido a este tipo de redes possuir uma menor latência e maior largura de banda, não tendo tanta necessidade de priorizar ligações.

7.19 Pergunta 19)

O uso de tramas Request To Send e Clear To Send, apesar de opcional, é comum para efetuar "pré-reserva"do acesso ao meio quando se pretende enviar tramas de dados, com o intuito de reduzir o número de colisões resultante maioritariamente de STAs escondidas. Para o exemplo acima, verifique se está a ser usada a opção RTS/CTS na troca de dados entre a STA e o AP/-Router da WLAN, identificando a direccionalidade das tramas e os sistemas envolvidos. Dê um exemplo de uma transferência de dados em que é usada a opção RTC/CTS e um outro em que não é usada.

8519	73.544155	HitronTe_f3:9a:46 …	AzureWav_0f:0e:9b …	802.11	76	Request-to-send, Flags=........C
8520	73.544159		HitronTe_f3:9a:46 …	802.11	72	Clear-to-send, Flags=........C
8521	73.544163	76:9b:e8:f3:9a:43	AzureWav_0f:0e:9b	802.11	444	QoS Data, SN=2, FN=0, Flags=.p....F.C
8522	73.544167	AzureWav_0f:0e:9b …	HitronTe_f3:9a:46 …	802.11	68	802.11 Block Ack, Flags=........C
8523	73.544170	HitronTe_f3:9a:46 …	AzureWav_0f:0e:9b …	802.11	76	Request-to-send, Flags=........C
8524	73.544174		HitronTe_f3:9a:46 …	802.11	72	Clear-to-send, Flags=........C
8525	73.544215	76:9b:e8:f3:9a:43	AzureWav_0f:0e:9b	802.11	282	QoS Data, SN=0, FN=0, Flags=.p..R.F.C
8526	73.544219	AzureWav_0f:0e:9b …	HitronTe_f3:9a:46 …	802.11	68	802.11 Block Ack, Flags=........C

Figura 7.19.1: Uso de RTS/CTS no envio da trama 8521.

Como podemos verificar na figura 7.19.1, foi utilizado tramas *Request to Send* e *Clear to send* para reservar o meio. Como sabemos da pergunta anterior, a trama 8521 veio de um dispositivo externo à rede, logo o *AP HitronTe* enviou uma trama *Request-to-send* para o dispositivo *AzureWav* enviado de imediato uma trama *Clear-to-send* (tramas 8519 e 8520). A seguir foi transmitida a trama 8521 e a seguir o dispositivo *AzureWav* enviou uma trama do tipo *Block Ack* a sinalizar que recebeu múltiplos blocos de informação e quais as possíveis tramas que poderão ter sido mal recebidas. Verificamos que existiu a possibilidade da trama ter sido mal transmitida devido à trama ter sido reenviada(tramas 8523 até 8526).

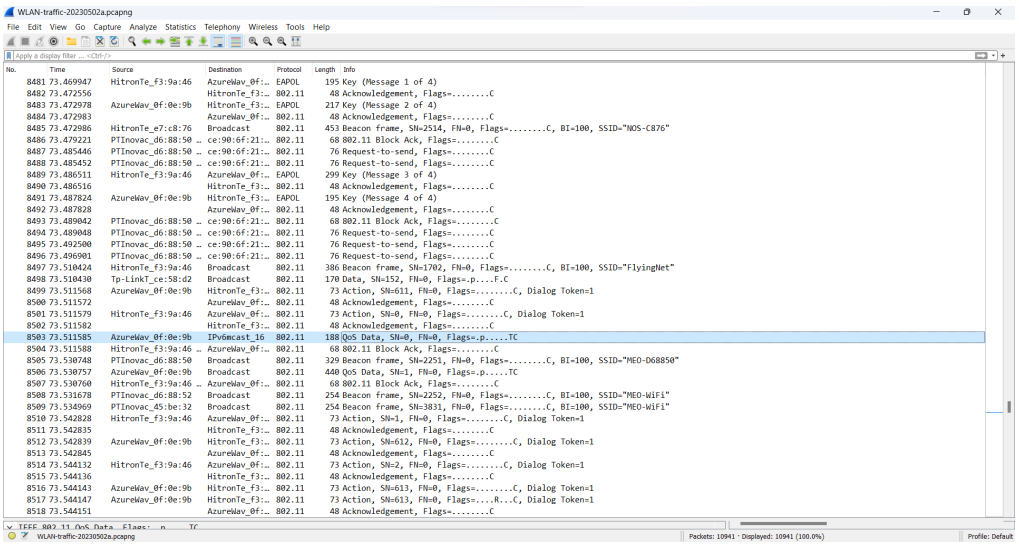

Figura 7.19.2: Captura Trama *Wireshark* onde não se verifica o uso de *RTS/CTS*

Como podemos observar na figura 7.19.2, a trama de ordem 8503 possuí o mesmo *subtype* da trama da figura 7.19.1 (*QoS Data*) não havendo um pedido de *Request-to-Send* anteriormente, logo, esta trama não utiliza o método *RTS/CTS*.

Capítulo 8

Conclusão

Na realização deste trabalho prático tivemos a oportunidade de estudar sobre os temas *Acesso Rádio, Scanning Passivo e Ativo, Processos de Associação* e *Transferência de Dados*.

Novamente, aprofundamos os nossos conhecimentos de *Wireshark*, mais especificamente recorrendo a aplicações de filtros e análise de tramas *IEEE 802.11*.

Concluindo, conseguimos aplicar na prática o conhecimento adquirido tanto nas aulas teóricas como nas aulas práticas. Além disso, tivemos a oportunidade de reforçar os nossos conhecimentos acreditando ter alcançado os objetivos propostos e superado todos os desafios encontrados.